(12) **UK Patent Application** (19) **GB** (11) **2 268 605** (13) **A**

(43) Date of A Publication 12.01.1994

(21) Application No 9313094.6

(22) Date of Filing 24.06.1993

(30) Priority Data
(31) 2073495 (32) 08.07.1992 (33) CA

(71) Applicant(s)
Mitel Corporation

(Incorporated in Canada - Ontario)

PO Box 13089, Kanata, Ontario K2K 1X3, Canada

(72) Inventor(s)
Michael M.W. Wright
Henry K Ting
David James Boshard

(74) Agent and/or Address for Service
John Orchard & Co
Staple Inn Buildings North, High Holborn, LONDON, WC1V 7PZ, United Kingdom

(51) INT CL5
G06F 1/00 12/14

(52) UK CL (Edition M)
G4A AAP
U1S S2214 S2215

(56) Documents Cited
GB 2228807 A   US 5058162 A

(58) Field of Search
UK CL (Edition L) G4A AAP
INT CL5 G06F 1/00
ONLINE DATABASES : WPI, COMPUTER DATABASE, COMPUTER ASAP

(54) Option selection and control.

(57) A method of enabling functional options in a computer system by selecting codes corresponding to the desired functional options, combining the codes and the serial number of the system to obtain a combined option code, receiving a password for enabling functional options corresponding to the selected codes, processing the password through a function to obtain a resultant password, comparing the resultant password with the combined options code, and enabling the desired functional options corresponding to the selected codes if the resultant password and the combined options code are the same.
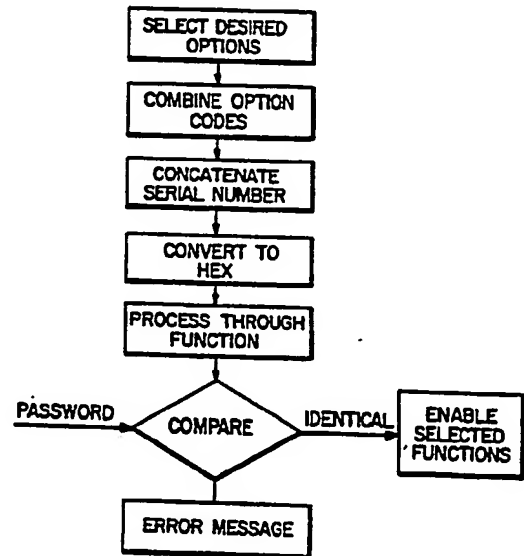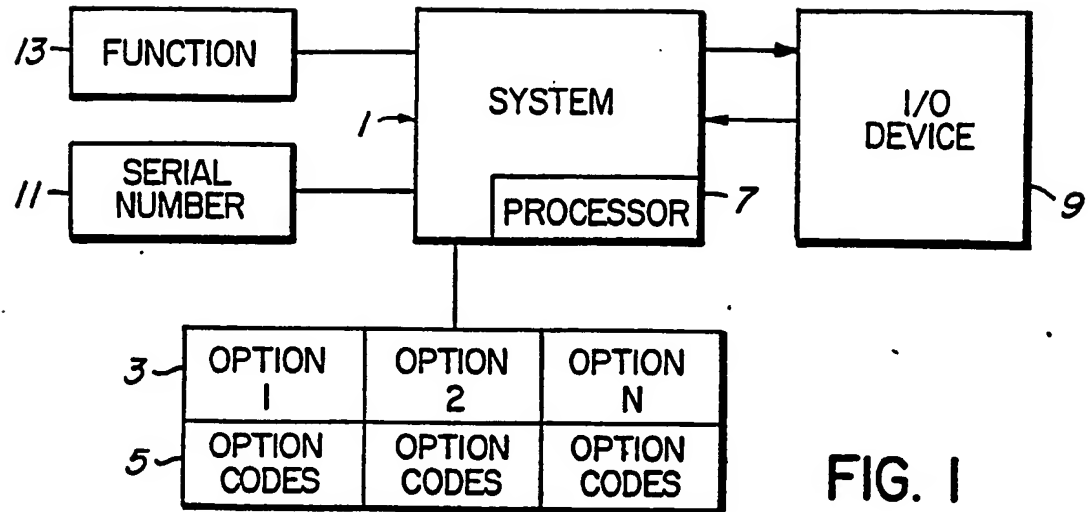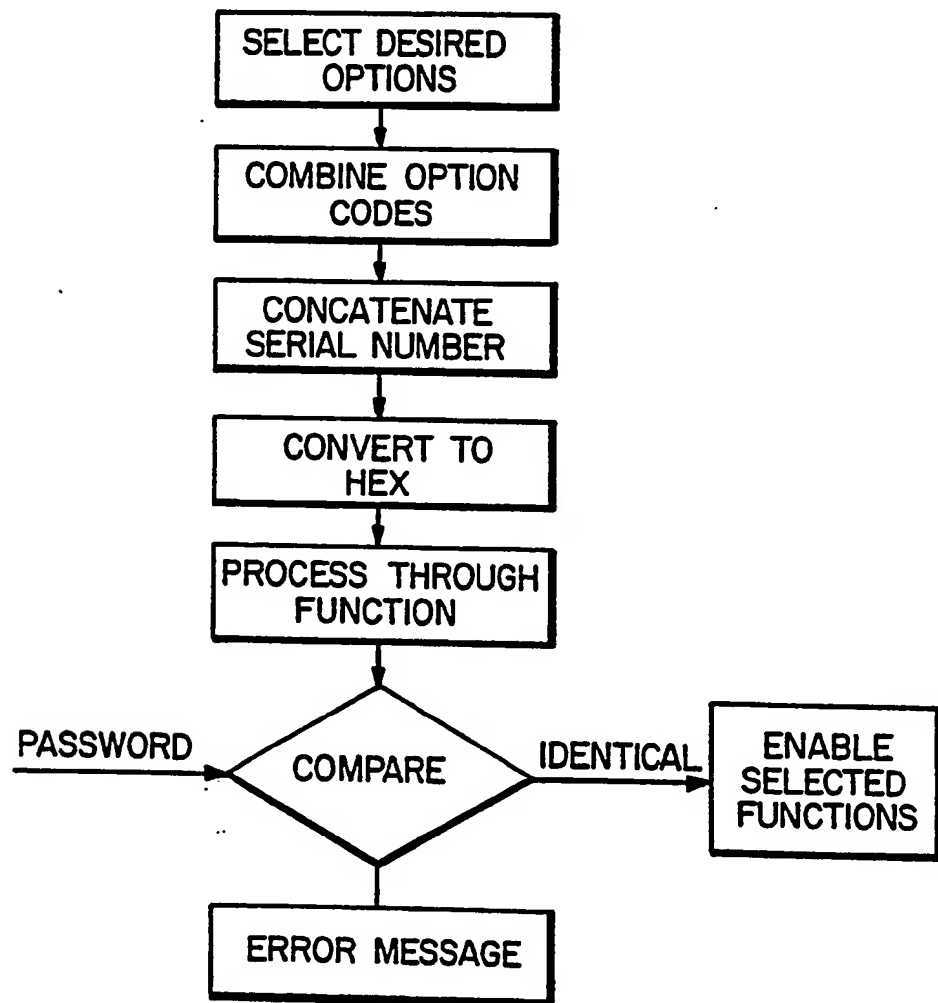

FIG. 2

GB 2 268 605 A

FIG. 1

FIG. 2

OPTION SELECTION AND CONTROL

This invention relates to a method of providing functional options to purchasers of computer type systems such as a telephone switching system.

A purchaser of a computer type system such as a telephone switching system often purchases the system with certain optional features, but later wishes to add to them. Such features have been provided by selling hardware modules or software upgrades. However such means for adding options is cumbersome, since the supplier must estimate the likely number of upgrades to be purchased within a reasonable future time, and which upgrades are likely to be purchased, and then manufacture and stock hardware option modules or floppy disks carrying software upgrades for those options. In addition, hardware and software piracy of the modules or software is also a large problem and difficult to detect and to stop.

A method will be described of providing options for computer type systems without requiring any stocking of hardware modules or software floppy disks and which virtually eliminates the problem of piracy. The problems of predicting and premanufacturing the quantity and types of options are thus totally eliminated, eliminating the significant cost of producing the option hardware modules or floppy disks, of transport of such items from the supplier, and of the staff required to deal with the manufacture, stocking and transportation of them. Yet any one or plural options can be provided rapidly and securely.

In a particular embodiment to be described options are provided with the original system, but the options are inhibited from being enabled until options

are purchased from the supplier. Once the options have been purchased, the supplier provides a computed code which corresponds to the desired options, the code being referred to herein as a password.

In one embodiment, codes corresponding to the desired options are combined together and combined with the serial number of the system. The combination is processed through a function means, and the result is compared with the password. If the two are identical, the selected options are enabled.

In another embodiment, the password is passed through a function means and the result compared with the combined codes. If the two are identical, the selected options are enabled.

Thus the computer system preferably contains a serial number which is readable by software. Each possible option which is provided with the computer system must contain an unique code. That unique code is either embodied in hardware or firmware readable by software, or is contained in software, depending on how the system operates. Each of the functional options, whether embodied in hardware or software is latent until it is enabled.

The function can be embodied in hardware, firmware or software, and can be any function, but should be a function that is most difficult to figure out. Preferably the knapsack encryption algorithm is used, which has been proven theoretically to be an intractable algorithm. The algorithm utilizes a key which is known only to the vendor of the options, and theoretically cannot be figured out in an amount of time which is described by a polynomial function (which describes an exponential amount of time). It is thus virtually impossible for a pirate to duplicate the enabling passwords, each enabling password for each

group of desired functional options for each serial
numbered computer type system being different and is
virtually impossible to duplicate.

Because the purchaser communicates only
information to the supplier and the supplier
communicates only information by return, the desired
options can be enabled very quickly, and indeed can be
effected automatically between computer systems, once
there is verification of payment or the acceptance of an
order. The supplier need only have a computer system
which generates a password which can be entered into the
computer type system in which the selected type options
are to be enabled.

In accordance with an embodiment of the
invention, a method of enabling a functional option in a
computer type system is comprised of storing a serial
number which is specific to the system, storing
different codes each corresponding to a possible
functional option which can be enabled in the system,
selecting codes corresponding to desired functional
options, combining the selected codes and the serial
number to obtain a combined option code, receiving a
password for enabling functional options corresponding
to the selected codes, processing the password through a
function apparatus or process to obtain a resultant
password, comparing the resultant password with the
combined options code, and enabling the desired
functional options corresponding to the selected codes
in the event the resultant password and the combined
options code are the same.

In accordance with another embodiment of
the invention, a method of enabling a functional option
in a computer type system is comprised of storing a
serial number which is specific to the system, storing
different codes each corresponding to a possible

functional option which can be enabled in the system, selecting codes corresponding to desired functional options, combining the selected codes and the serial number to obtain a combined option code, processing the combined option codes through a function apparatus or process to obtain a resultant options code, receiving a password for enabling functional options corresponding to the selected codes, comparing the resultant options code with the password, and enabling the functional options corresponding to the selected codes in the event the resultant options code and the password are the same.

In accordance with another embodiment of the invention, a method of providing a functional option in a computer type system is comprised of providing a computer type system with a plurality of options already provided, but inhibited from operating, selecting certain desired ones of the options, entering a code into the system, and enabling the selected options upon receipt of the code.

An embodiment of the invention will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 is a block diagram of a system in which the method can be carried out, and

Figure 2 is a flow chart showing steps in a preferred embodiment of the invention.

A computer type system 1 is purchased by a buyer from a vendor. The computer type system includes all of the possible functional options 3 that can be implemented on the system, shown as option 1, option 2...option N. These options 3 can be implemented as

hardware modules or as software program processes.
However it is important that each of the functi nal
options should have its own distinct option code, shown
in Figure 1 as option codes 5.

5   The option codes can be read by a processor 7
which is part of the system 1, from each functional
option, e.g. realized as firmware associated with each
hardware module, as some other wired code such as
designated by option switches, associated with each
10   hardware module, as a stored number associated with each
program implementing a particular functional option, or
they may be stored in a table in a memory of system 1.

      A table of example internal codes stored in
association with each option is shown in Table 1 below.

15

Option	Internal Codes	Selected Codes
A	0000000000000001	
B	0000000000000010	0000000000000010
C	0000000000000100	0000000000000100
D	0000000000001000	0000000000001000
E	0000000000010000	
F	0000000000100000	0000000000100000
G	0000000001000000	
H	0000000010000000	
I	0000000100000000	
J	0000001000000000	0000001000000000
K	0000010000000000	
L	0000100000000000	0000100000000000
M	0001000000000000	
N	0010000000000000	
O	0100000000000000	
P	1000000000000000	

TABLE 1

      Let us assume that the system buyer wishes to
purchase options B, C, D, F, J and L.

      The buyer accesses the table or otherwise
40   designates the particular options by means of an
input/output device 9 which can be, for example, a

terminal display and keyboard. A dialog box or form is shown on the display with all of the possible options, and if, desired, the associated option codes which the computer system retrieves from the firmware, hardware or

5   functional option programs.

The user then selects the particular options desired. The options can be, e.g. for a telephone system, Advanced Data, DPNSS, visually handicap operator console, etc. On some systems there could be e.g.

10   ninety options available. All options are provided with the original purchase of the system, but are latent and not able to be enabled by the system.

With the selection of particular options, the corresponding internal option codes 5 are distinguished,

15   e.g. as shown in the third column of Table 1, "Selected Codes". It is preferred, although it is not mandatory, that the internal codes should be of binary type.

This completes the first step in the process shown in Figure 2.

20   The computer system 1 then combines the option codes e.g. by adding. For the selected code shown in Table 1, the following combined option code is produced:

0000101000101110

A software readable serial number 11 (Figure

25   1) is associated with computer system 1. This serial number can be in a software readable hardware module, firmware, or can be contained in software. The serial number should be unique to each individual system sold.

The serial number is then combined with the

30   combined option code, preferably by concatenation. For example if the system identifier was 632 or 0000001001111000 in binary:

0000001001111000 | 0000101000101110

yields   00000010011110000000101000101110101011

The combined code is converted into HEX, and is 02780A2E.

This combined code in HEX is provided to the options vendor along with payment or arrangements for payment for the options represented by the code.

The vendor provides a password in response. This password is created by the vendor by processing the options code provided to it by the buyer through a function apparatus or process. The apparatus can be a software or a hardware operator. In the present example f(02780A2E)=F5J790, the number F5J790 is the password which the vendor provides to the buyer.

The function f can be any function, but it should be a function which is very difficult to figure out. It is preferred that the function should be based upon the knapsack encryption algorithm, which has been proven in theory to be an intractable algorithm. The algorithm utilizes a key which is only known to the vendor.

A function apparatus or process 13 is also provided in the system, which can operate on a number given to it. The function processed in the function apparatus or process 13 can be identical in all of the systems sold by the vendor, and must process a number in an identical manner to that by the vendor.

The buyer, receiving the password from the vendor enters it via I/O device 9 into the system, which computes a resultant code by operating on the password utilizing the function of function apparatus or process 13. Thus with the entering of the password F5J790, according to one function the result after processing through the function is f(02780A2E), which is the HEX code noted above.

The computer system then causes a comparison of the HEX combined code resulting from the addition and

concatenation of the selected codes and serial number,
and the code resulting from the processing of the
password through the function. The resulting HEX
numbers 02780A2E should be the same. If they are the

5   same, the selected options are enabled. If they are not
the same, no options are enabled, and an error message
can be indicated on the I/O device 9.

Since it is virtually impossible to determine
what key has been used by the vendor, it is virtually

10   impossible to pirate the enabling or operation of the
options in association with the system.

While it is preferred that the processing
should occur in binary and HEX, it will be understood
that other number bases can be utilized.

15   A person understanding the above description,
may now conceive of variations or other embodiments.
For example, rather than processing the password through
a function in the system to obtain a resultant code
which is compared with the combined code, the combined

20   code can be processed through the function to obtain a
resultant password which is compared with the password
received from the vendor.

These and all other embodiments utilizing the
principles of this invention are considered to be part

25   of this invention as defined in the claims appended
hereto.

CLAIMS

1. A method of enabling a functional option in a computer type system comprising:

   (a) storing a serial number which is specific to said system,

   (b) storing different codes each corresponding to a possible functional option which can be enabled in said system,

   (c) selecting codes corresponding to desired functional options,

   (d) combining said selected codes and the serial number to obtain a combined option code,

   (e) receiving a password for enabling functional options corresponding to said selected codes,

   (f) processing the password through a function to obtain a resultant password,

   (g) comparing the resultant password with the combined options code,

   (h) enabling the desired functional options corresponding to said selected codes in the event the resultant password and the combined options code are the same.

2. A method as defined in claim 1 in which the selected codes are combined by addition.

3. A method defined in claim 2 in which the combined selected codes are combined with the serial number by concatenation.

4. A method as defined in claim 1 in which the function is comprised of an encryption means or process.

5. A method as defined in claim 4 in which the encryption means or process is an encryption algorithm processed by a processor of the computer type system.

6. A method as defined in claim 5 in which each of the codes is a binary number and in which the serial number is a binary number.

7. A method as defined in claim 6 including converting the combined options code into HEX, and in which the resultant password is in HEX.

8. A method as defined in claim 7 in which the selected codes are combined by addition and the serial number is combined with the added selected codes by concatenation.

9. A method of enabling a functional option in a computer type system comprising:

(a) storing a serial number which is specific to said system,

(b) storing different codes each corresponding to a possible functional option which can be enabled in said system,

(c) selecting codes corresponding to desired functional options,

(d) combining said selected codes and the serial number to obtain a combined option code,

(e) processing said combined options codes through a function means to obtain a resultant options code,

(f) receiving a password for enabling functional options corresponding to said selected code,

(g) comparing the resultant options code with the password, and

20   (h) enabling the functional options corresponding to said selected codes in the event the resultant options code and the password are the same.

10. A method as defined in claim 1 including the step of providing said combined options code to a vendor, processing said combined options code by said vendor through a vendor function using

5   the same function as the computer type system, and obtaining said password thereby.

11. A method as defined in claim 9 including the step of providing said combined options code to a vendor, processing said combined options code by said vendor through a vendor function using

5   the same function as the computer type system, and obtaining said password thereby.

12. A method as defined in claim 10 wherein the function is comprised of a knapsack encryption algorithm.

13. A method as defined in claim 11 wherein the function is comprised of a knapsack encryption algorithm.

14. A method of providing a functional option in a computer type system comprising:

(a) providing a computer type system with a plurality of options already provided, but

5   inhibited from operating,

(b) selecting certain desired ones of said options,

Pat nts Act 1977.
Examin r's rep rt to the Comptroller under
Secion 17 (The Search Report)

Application number	GB 9313094.6

Relevant Technical fields

(i) UK Cl (Edition L)   G4A (AAP)

(ii) Int Cl (Edition 5)   G06F 1/00

Databases (see over)
(i) UK Patent Office

(ii)   ONLINE DATABASES: WPI, COMPUTER DATABASE, COMPUTER ASAP

Search Examiner	S J PROBERT
Date of Search	29 JULY 1993

Documents considered relevant following a search in respect of claims   1-13, 23

Category (see over)	Identity of document and relevant passages	Relevant to claim(s)
X	GB 2228807 A (ESSETTE LETRASET LTD) see whole document	1, 4-7 9-13
X	US 5058162 (SANTON ET AL) see particularly column 7 line 50 to column 8 line 24	1, 4-7 9-13

Category	Identity of document and relevant passages	Relevant to claim(s)

Categories of documents

X: Document indicating lack of novelty or of inventive step.

Y: Document indicating lack of inventive step if combined with one or more other documents of the same category.

A: Document indicating technological background and/or state of the art.

P: Document published on or after the declared priority date but before the filing date of the present application.

E: Patent document published on or after, but with priority date earlier than, the filing date of the present application.

&: Member of the same patent family, corresponding document.

Databases: The UK Patent Office database comprises classified collections of GB, EP, WO and US patent specifications as outlined periodically in the Official Journal (Patents). The on-line databases considered for search are also listed periodically in the Official Journal (Patents).